Guida di Kalidor all'hacking per Win95/98 v2.2

Indice:

Disclaimer:

Usa queste informazioni a TUO rischio e pericolo. Io (Kalidor) e qualsiasi altra persona mi abbia aiutato a scrivere questa guida non si assumerà NESSUNA responsabilità per l'uso, l'utilizzo o l'abuso di questo testo. Le seguenti informazioni sono state scritte SOLAMENTE per scopo educativo e informativo e NON possono essere usati per scopi illegali. Leggendo questo file tu accetti i seguenti termini:
Comprendo che usare le seguenti informazioni è un atto illegale. Capisco e accetto di essere il SOLO responsabile delle mie azioni. Se vengo messo nei guai da queste informazioni NON incolperò o tirerò nei guai colui (Kalidor) che ha scritto questo testo o ogni altro suo collaboratore o qualsiasi altra persona mi abbia dato questo file. Io capisco che le informazioni qua contenute sono SOLO per scopo di educazione. Questo file può essere usato per controllare la sicurezza del TUO sistema.

Inoltre per leggere questo testo devi possedere un'automobile rosa e avere almeno 154 anni.

Introduzione:

Grazie per avere scelto la "Guida di Kalidor all'hacking per Win95/98". Se non hackerete un server in 3 settimane avrete i vostri soldi indietro.

Benvenuti alla mia guida. Questa guida è stata fatta appositamente per quelli che l'hacking non sanno nemmeno cosa sia (o quasi) e che non hanno mai sentito parlare di linux, unix o robe simili.
Per i profani l'hacking è l'atto di penetrare nei sistemi trovando la password per il login più privilegiato possibile (login e password spiegati dopo). Voi penserete che queste cose si vedono solo nei film di fantascienza e invece NO! Ed è incredibilmente facile hackerare. Naturalmente bisogna avere alcune conoscenze sui computer se no non sarà molto facile per voi. Questo è quello che dovete sapere prima di iniziare:

Requisiti di sistema:

- Una buona conoscenza dell'inglese altrimenti sarete spacciati
- Un po' di dimestichezza coi computer ed un po' di autonomia, ad esempio capire come funziona un programma senza l'aiuto di qualcuno (magari leggendo il manuale o il readme)
- Una buona dose di fortuna. Se siete sfigati come Paperino lasciate stare (scherzo=))
- Non avere assolutamente fifa di commettere atti...illegali
- Non essere persone generose e di buon cuore=). Bisogna essere MALEFICIIII MUAHAAHAHAAAA (non è detto poi...=)
- Avere voglia di fondersi il cervello e stare ore e ore e giorni a provare, riprovare, ririprovare...diventare rincoglioniti...etc etc
- Essere maniaci del computer. Se pensate che il computer è uno strumento come un altro lasciate stare...io do I NOMI ai computer (sto scrivendo con la mia Arcady;-)

Bene avete controllato i punti scritti sopra? Siete a posto? QUASI a posto? Ok cominciamo.

Parte teorica:

E così comincia la (pallosissima) parte teorica. Vi consiglio VIVAMENTE comunque di leggerla perchè se passate subito alla parte pratica ho paura che non capirete molto; nella parte pratica io do' perscontato che abbiate letto questa parte o che sappiate già quello che c'è scritto qui.
Spegnete le luci, staccate il telefono, chiudete le finestre...no che poi non ci vedete un kakkio, buttate fuori a calci la ragazza...cominciamo.

Unix:

Lo unix (in inglese si legge iùnics=) e il linux (la sua versione free) sono i sistemi operativi più importanti in internet poiché sono stati progettati su questa base. Lo unix è stato fatto appositamente per le reti (internet & intranet). Per imparare ad hackerare dovete conoscere bene questo sistema operativo; per consolarvi vi dico che è simile al DOS come comandi (ma mooooooolto più flessibile – e più difficile).
Quando vi connettete ad un server (come fare è spiegato dopo) sarà quasi sicuramente unix o linux. Una volta connessi (sia con ftp o con telnet, spiegato dopo pure questo) vi verrà detto:

Unix (o linux) Version blablabla on server.hackeroso.com at gg:oo:mm

Login:

Ecco questa è la famosissima domanda immancabile in tutti i server. Il login è il nome che usate per identificarvi quando vi connettete a qualcosa. Nel server ci sono vari login in memoria. A seconda di quale login mettete il server vi darà più o meno privilegi nel sistema. Poi il server vi chiederà:

Password:

Questa è la password (parola chiave) che uno user (utente) associa al suo login. Quando la scrivete non vedrete niente per ragioni di sicurezza. Non vedrete neanche gli asterischi perchè questi determinano la lunghezza della password e ciò è fondamentale nello unix. Se sbagliate il login o la password vi verrà detto:

Login incorrect.

Login:

Ciò per tutti gli hacker è molto antipatico. Se invece la password e il login li beccate il server vi dirà:

Last login on server.blabla.com at gg:mm:aa.

You have mail / No mail. (non essenziale)

% (oppure:)
$

Questi due caratteri compaiono, seguiti alcune volte da dei commenti del sysop (il proprietario del server) quando entrate con un login normale. Quando invece entrate con un login a pieni poteri, di solito il login "root", vi verrà scritto:

#

Attenzione, alcune volte (ma molto raramente), i sysop possono mettervi questo carattere per farvi credere di essere dei root e farvi pensare che potete fare quel che vi pare. Comunque questo è il simbolo che rappresenta gli user a pieni poteri.
Ecco ora i comandi più comuni che potete usare una volta entrati (attenzione, unix e linux sono CASE SENSITIVE, ciò vuol dire che maiuscolo e minuscolo non sono la stessa cosa, ad esempio pirla, PIRLA, Pirla, PiRlA e plrLa sono tutte cose diverse. Comunque generalmente in unix quasi tutto è minuscolo):
ls: da la lista dei file. In pratica è come il DIR /w. Se volete potete scrivere anche:
ls -al: questo vi da la lista uguale al comando DIR e vi mostra anche i file nascosti
cd: change directory. Cambia la directory.. è il CD del DOS. Attenzione però: se volete fare un cd.. dovrete scrivere cd .. CON LO SPAZIO in mezzo.
vi: è come l'EDIT ma e' difficile da usare; io uso PICO che è più versatile, purtroppo non si trova su tutti i sistemi quindi è utile conoscere anche VI.
mail: legge la mail associata al login che usate. Per avere i comandi della mail scrivere ?.
rm: uguale a DEL. Cancella i file.
cp: come COPY.
mv: come REN.
pwd: vi dice la directory in cui vi trovate.
write: è una specie di chat. Usate write nomelogin.
man: il manuale. Usate man comando.
cc: compilatore c.
chmod: cambia i diritti di accesso di un file. Spiegato dopo.

Quando entrate con uno user specifico, ad esempio kalidor, avrete certi privilegi. Questi privilegi sono configurati nel passwd file, localizzato in /etc/passwd (passwd è un file senza estensione, negli unix sono comuni). Ora scrivete:

$pwd
Current directory is /
$cd etc
$vi passwd

root:wXU9dj5HgegfY:0:root:/root:/bin/bash
casttwo:JauyqjalnO4r.:100:Claudio:/usr/local/WWWCAST:/bin/bash
alex:DnC3.8ki/Vxbg:100:Alessandro:/usr/local/WWWCAST:/bin/bash
drago:PhQ93Kkb3uKWk:100:drago:/usr/local/WWWDRAGO:/bin/bash
erreti:Ac94JrWgDUE5s:100:erreti:/usr/local/WWWERRETI:/bin/bash
ma:526W/EMJtPS0I:100:Angelo:/usr/local/WWWWORLDC:/bin/bash
kalidor:oLi8fwrShd/YA:100:KALIDOR:/usr/local:/bin/bash
persyst:PjZQgViux0.RY:100:persyst:/usr/local/WWWPERSYST:/bin/bash
ivars:CpQzohSaJAyeg:100::/usr/local/WWWIVARS:/bin/bash
sqcons:Oa3n.7A28gXaM:100::/usr/local/WWWSQCONS:/bin/bash
serte:Bcxzo18l4L0AU:100::/usr/local/WWWSERTE:/bin/bash

ivar:D8elXPHyo4LgY:100::/usr/local/WWWIVAR:/bin/bash

Bene. Che cacchio è 'sta roba??? E' il file che contiene le PASSWORD per gli user. Prendiamo il mio login:

kalidor:oLi8fwrShd/YA:100:KALIDOR:/usr/local:/bin/bash

kalidor è il nome del login, oLi8fwrShd/YA è la password (naturalmente criptata, come decriptarla spiegato dopo), 100 è il livello di permission, KALIDOR è la descrizione del login, /usr/local è la directory di partenza e /bin/bash è il tipo di unix che state usando. Il vostro obbiettivo è di avere la password per lo user con privilegio 0 (qui, e in quasi tutti i server, è il root). In certi casi alcuni o tutti i login possono essere così:

```
sider:*:100::/usr/local/WWWSIDER:/bin/bash
```

* significa che la password è SHADOWED e che quindi non è decriptabile, a meno che non si possa leggere il file etc/shadow che contiene le password shadowed. Questo file però è accessibile soltanto dal root o da un login 0.

Ora scriviamo ctrl-z per uscire e facciamo:

```
$pwd
Current directory is /etc/
$ls -al
total 4
drw-r--r-- 2 0    1      96 Apr 18 1997 .
drw-r--r-- 2 0    20     96 Apr 18 1997 ..
-rw-r--r-- 2 1    1      96 Apr 18 1997 passwd
-rw-r--r-- 2 1    1      96 Apr 18 1997 group
```

Che cosa sono quella roba dwr-r-r e le altre simili? Sono le permission per il file. d vuol dire directory, r vuol dire read (leggere), w vuol dire write (scrivere) e x vuol dire execute (eseguire). Quando c'è un - vuol dire che la certa cosa che dovrebbe stare lì non si può fare. La sequenza di permission completa è drwxrwxrwx. Dopo la d il primo gruppo di tre lettere è associato al root, quindi -rw-r--r-- vuol dire che il root può leggere e scrivere quel file. Il secondo gruppo di tre lettere è associato al gruppo, cioè l'insieme di login che ha un certo privilegio (i vari gruppi si possono vedere in etc/group e se stai in un login joinabile da un gruppo senza password usa il comando chgrp). L'ultimo gruppo di tre lettere è associato allo user normale.
Ora sapete le cose principali sullo unix.

IP, Porte & Protocolli:

Ci sono vari modi di accedere ad un server. Con il browser, con ftp, con telnet e con altre cose. Quando si ci connette ad un server il programma che state utilizzando analizza il nome del server (ad esempio www.microsoft.com oppure 210.75.4.13) e se è scritto in formato letterale lo converte con il DNS, un programma che gira in vari server nelle reti (chiamati name servers) e che converte da letterale a numerico e da numerico a letterale. Ad esempio www.microsoft.com corrisponde a 207.46.131.137. Questo numero è l'idinteficazione del server e in ogni sezione (separate dal .) possono stare da 1 a 3 numeri. Questo codice si chiama IP (Internet Protocol). Ora per scegliere in che modo entrare si usano le PORTE. Ogni programma usa una porta diversa per connettersi. Ecco le porte più comuni:

Porta	Utilizzo
7	echo (ping- solo via ICMP)
21	ftp (File Transfer Protocol)
23	telnet
25	stmp (Simple Mail Transfer Protocol)
79	finger
80	http (Hyper Text Transfer Protocol
110	pop3 (Post Office Protocol 3.x)

Per connettersi a queste porte ci sono 3 modi:

TCP: quello classico che usano tutti (Transfer Control Protocol)
UDP: per spedire pacchetti e dati speciali (User Datagram Protocol)
ICMP: per spedire pacchetti PING per testare la velocità tra due computer (Internet Control Message Protocol)

Programmi utili:

I programmi per win95/dos che probabilmente vi serviranno ad hackerare sono:
Netinfo: per avere più informazioni possibili da un server
GenerID: per generare identità false con codice fiscale per registrarvi nei provider
John the Ripper: per decriptare i passwd file
Back Orifice: per rubare le password degli account ad un altro per mezzo di un trojan horse
UnSecure: programma per provare password su un dato login molto velocemente
Qualche codice C per sniffare (spiegato dopo).
Questi programmi sono disponibili alla mia home page http://members.xoom.com/Kalidor_hp/secret.html
La password come trovarla è spiegato nella sezione "Come hackerare le password in javascript".

Precauzioni:

Quando hackerate c'è sempre una possibilità che vi scoprano e che dal vostro IP risalgano alla vostra identità. Perciò quando hackerate dovete SEMPRE usare un account per internet NON VOSTRO. Per ottenerlo ci sono due modi:
1) Registrarsi ad un provider (telefonando) usando GenerID e dando i dati generati. Vi daranno un account provisorio di due settimane, da aggiornare ogni volta che scade con lo stesso metodo. Questo è il metodo più fastidioso perchè ogni 2 settimane bisogna telefonare.
2) Rubare l'account a uno che sapete che internet non lo usa spesso. Per fare questo usate Back Orifice. Mandate il file boserve.exe alla vittima e con qualche scusa glielo fate eseguire. Poi lanciando BoGui e usandolo su di lui avrete accesso alle sue password di account.
Ci sono anche dei programmi che vi danno una certa sicurezza in quanto a rintracciamento: gli spoofers che falsificano il nome del vostro pc su irc e ftp, e i jammer che non ho ancora capito cosa facciano e se funzionano ma sembra che vi diano ulteriore privacy.

Ulteriori precauzioni vanno prese dentro il sito. Prima di tutto non bisogna cancellare o danneggiare nessun file, tranne quelli di log e passwd, altrimenti è più probabile che, nel caso veniate beccati, vi arrestino. Inoltre non hackerate mai questi tipi di server:
.GOV (siti di governo MOLTO pericolosi in quanto a sicurezza)
.MIL (siti militari ANCORA PIU' pericolosi)
e qualsiasi server molto importante che amministra più di un milione di utenti internet (come le backbone).
Inoltre non praticate MAI lo spionaggio industriale. Hackate per divertimento, non per soldi, altrimenti finirete presto in galera o in una sperduta casa in Finlandia dove andrete per non farvi beccare.

Parte pratica:

Eccoci alla parte pratica. Qui imparerete a fare dei semplici hackeraggi. Spero che abbiate letto la parte teorica altrimenti qui non capirete un kakkio=).

Come hackerare in Win95:

In molte guide per gli hacker c'è scritto che se non hai linux o unix non puoi fare niente. Ciò non è assolutamente vero. Con win95 è possibile hackerare quasi facilmente come usando linux. Naturalmente avrete bisogno di alcuni programmi specifici e di qualche account per linux (detto shell account, spiegato dopo). L'unico problema di win95 sono i bug. Win95 è pieno di bug e ciò può impedire molto l'hacking; ad esempio su win95 non si può usare S.A.T.A.N. poichè i protocolli di rete di win sono programmati un po' alla cacchio e satan ha bisogno di protocolli veloci e programmati in modo da ottimizzare la connessione. Inoltre molti script per c possono essere lanciati solo da linux. A questo inconveniente si può rimediare agendo attraverso dei computer linux remoti, hackerati da voi. Comunque anche se in win95 tutto forse sarà un po' complicato non è mai impossibile, basta sapersi arrangiare. Ma se potete procurarvi linux, FATELO.

Entrare nei server:

Questa è la prima e più difficile parte dell'hacking. Per entrare nei server bisogna prima di tutto avere più informazioni possibili su di esso. Quindi aprite netinfo o un prog simile e fate tutto quello che potete fare li. La funzione più importante in netinfo è il FINGER. Esso ti permette di vedere tutti i login connessi al server al momento e darvi informazioni sui login che non sono connessi. Per usarlo prima di tutto fingerate @server.da.hackare (potete anche farlo usando un prog per connettersi ad una porta specifica...andate sulla porta 79 e scrivete invio per gli user online o il nome dello user che volete se è offline). Se vi dice che non può connettersi allora niente. Se invece vi da qualche login o vi dice "no one logged on" allora il server ha il finger attivato. Ora prendete nota dei login che vi da, se li da, e fingerateli singolarmente usando login@server.da.hackare. Vi darà informazioni più specifiche sui login in questione e forse anche altri login associati a quello che avete messo. Ora provate tutti i login che vi possono venire in mente e tutti quelli comuni (scritti dopo). Prendete sempre nota di questi login. Ora prendete nota di tutte le possibili password che avete ricavato con le altre funzioni del netinfo.
Adesso create un collegamento sul desktop di c:\windows\ftp.exe e lanciatelo. Questo è uno dei due programmi che si usano per connettersi ai server. Questo si connette alla porta 21. L'altro programma si chiama telnet.exe e sta anche in c:\windows\. Create un collegamento sul desktop anche di quello. Ftp (File Transfer Protocol) è il programa per trasferire i file da un computer all'altro e telnet è il programma che emula il vero unix. Quando si hackera bisogna usare tutti e due i programmi perchè con uno provate i login (provare i login con ftp da meno probabilità di essere beccati) e trasferite i file e con l'altro leggete le mail e modificate i LOG e i passwd (spiegato dopo) e fate molte altre cose. Ora che avete lanciato ftp vi chiederà per il login. Prendete uno dei login che avete fregato, oppure se non ci siete riusciti provate uno che pensate possa essere quello, e provate ad associarlo ad una password (abbastanza spesso accade che il login sia uguale alla password). Provate a combinare login e password in tutti i modi possibili. Ci sono tre tecniche per indovinare login e password:

*Login comuni:

Quando si compra un server e un computer in cui è installato linux o unix vi danno dei login e password di default, da modificare in seguito. Alcuni sysop ingenui non cambiano i login e password e se siete fortunati riuscite ad entrare senza molta fatica. Ecco i login di default:

LOGIN	PASSWORD
root	root, system, sysop, nomesistema, nomepersona, none, vedi sys
sys	sys, system, manager, nomedelsistema, vedi root
daemon	daemon, background, none
uucp	uucp, vedi guest
tty	tty
test	test
unix	unix, test
bin	bin, system, vedi root
adm	adm, admin, sys, vedi root
admin	adm, admin
sysman	sysman, sys, system
sysadmin	sysadmin, sys, system, admin, adm
who	who, none
learn	learn
uuhost	uuhost
guest	guest, user, anonymous, visitor, bbs, nomesistema / organizzazione
host	host
nuucp	nuucp, vedi uucp
rje	rje, none, vedi root
games	games, player
sysop	sysop
demo	demo, nomedelsistema, none
visitor	vedi guest
anonymous	vedi guest
anon	vedi guest
user	vedi guest

nomedelsistema	vedi guest
student	student, vedi guest
ftp	ftp, ftpuser, vedi guest
ftpuser	vedi ftp
xxcp	xenix
system	manager
nobody	nobody, none
field	service
archie	archie, none
qarchie	qarchie, none
whois	whois, none
bbs	nomedelsistema, bbs, waffle, none
services	nomedelsistema, services, none
info	nomedelsistema, info, none
new	nomedelsistema, new, none
newuser	nomedelsistema, newuser, none
ingres	none, ingres, nomedelsistema
date	date, none
lpq	lpq, none
time	time, none
weather	weather, forecast, none
forcast	vedi weather
help	help, none
test	nomedelsistema, test, none
waffle	vedi bbs
trouble	trouble, vedi root
lp	lp, printer, print, vedi root
unmountsys	unmountsys, unmount, vedi root
setup	setup, vedi root
makefsys	makefsys, vedi root
sysadm	sysadm, sys, system, vedi sys-adm-root
powerdown	powerdown, vedi root
mountfsys	mountfsys, vedi root
checkfsys	checkfsys, vedi root

*Password list:

Se ancora non siete entrati potete provare la tecnica del password list / brute force. Questa tecnica consiste di prendere un login che vi sembra debole e di provare a usare UnSecure su di esso, prima usando una password list e poi usando il metodo brute force. La password list è inclusa con unsecure e se non vi va bene ne potete trovare in giro con una piccola ricerca. Questo è il metodo più pericoloso però perchè con un grande numero di tentativi sullo stesso login c'è un alto rischio di essere beccati (sono sicuro che state usando il vostro account FALSO;-).

*Backdoors:

Le backdoor sono dei login speciali che un sysop (o un hacker, spiegato dopo) mette per far avere accesso a delle persone che non devono avere ufficialmente accesso al server oppure per avere un login di salvataggio con permission elevata nel caso si dimenticassero la password del root o in casi di emergenza. Se conoscete una persona che ha una backdoor nel server oppure avete preso una backdoor con il finger cercate di conoscere il più possibile su questa persona e cercate di scoprire la password. Provate anche il metodo delle password list su questo login qui.

Ricordate che entrare nel server è la parte più lunga e difficile quindi provate e riprovate e non scoraggiatevi, nessun server è inattaccabile.

Come avere l'accesso ROOT:

Bene qua siamo alla parte più importante dell'hacking. Avere l'accesso di ROOT. Prima di tutto andate a leggere il passwd file e vedete se il root è criptato o shadowato. Se è criptato prendete il file passwd, se è shadowato anche il file shadow; dopodiché usate john the ripper su tutti i login criptati e vedete quello che ne cavate fuori. Avrete ottenuto un paio di login. Se avete preso il root saltate con gioia per tutta la stanza. Se no provate a usare i nuovi login che avete fregato e vedete se riuscite a prendere informazioni sul login root. Ricordatevi che le password possono essere nascoste in ogni angolo del server tra le directory più anonime e insignificanti. Se ancora non avete preso il root allora mettetevi li con "john -i passwd" (vedi il manuale di john the ripper) e state li a crakkare per un paio di settimane e continuate a cercare bene nel server. Qualcosa troverete. Un'altro modo di trovare l'accesso di root è usando sniffer o exploits vari. Come usarli e quali sono è spiegato nella parte avanzata.

Come mantenere l'accesso al server:

Questa sezione, anche se non sembra, è molto importante dato che gli hackers principianti si fanno sgamare come novellini perdendo l'accesso root al server dopo un cambio di password. Mantenere l'accesso oltretutto è molto semplice. Ci sono tre cose da fare sempre.

- Crearsi una Backdoor. Quando si ottiene il root bisogna entrarci una volta sola altrimenti il sysop si potrebbe insospettire. Quindi quando si entra bisogna assolutamente crearsi una backdoor. Per far questo si edita il passwd file e si aggiunge NEL MEZZO del passwd (dico nel mezzo visto che così è meno probabile che il sysop se ne accorga) una stringa di questo genere: "kalidor::0:KALIDOR:/usr/local:/bin/bash". In questo modo la prossima volta che entrate al login scriverete kalidor e come pass non metterete niente
- Lanciare uno sniffer in background (come farlo spiegato dopo). In questo modo se cambiano la password di root potrete riprenderla per mezzo del log dello sniffer.
- Modificare sempre tutti i file di log in modo da non lasciare nessuna vostra traccia nel server. Come modificare i file LOG è spiegato dopo (no giuro ogni volta che dico "spiegato dopo" vuol dire che è DAVVERO spiegato dopo...tranquilli=)

Come hackerare le password in javascript:

Questo è l'hack più facile che io abbia mai fatto. Un esempio di password per javascript lo potete trovare alla mia home page (http://members.xoom.com/Kalidor_hp/secret.html) la cui password non la dico per non togliervi il piacere di trovarla=). Ci sono due tipi di password che potete trovare in un sito:

- Le password assegnate alle directory con un cgi-bin che sono quindi hackabili solo hackerando interamente il server
- Le password assegnate agli html con un codice javascript

Per hackerare queste ultime bisogna disporre di un programma capace di scaricare sull'hard-disk i file .htm / .html senza prima accedervi. Io consiglio GETRIGHT. Quindi andate alla mia home page, fate tasto destro su ENTER e fate copia collegamento. Ora scaricate il collegamento copiato con getright (per leggerlo fate ctrl-v, per copiarne uno usate ctrl-c). Ora che avete scaricato il file apritelo con il blocco note e leggete il codice html. Leggendo bene, anche se non conoscete l'html, troverete la password. Se per entrare nel sito con la password c'è un pulsante allora per sapere il link leggete l'html locale e poi eventualmente quello di destinazione. Ci sono dei casi in cui la password è scritta nell'html della pagina di partenza e in quel caso basta leggere l'html locale.

Parte avanzata:

Bene eccoci alla parte avanzata. Qua (almeno per me quando ho iniziato=) le cose diventano un po' più difficili. Questa parte è fatta per affinare le vostre tecniche di hacking e per permettervi di crearvi un vostro stile; ricordatevi che l'hacking è un'arte, se fatto bene, e non dev'essere trattato come uno strumento per fare il figo in mezza internet altrimenti non sarete più hacker ma la gente vi chiamerà lamer. Bene dopo una piccola cazziata cominciamo con la parte avanzata=).

Shell account:

La shell account è l'account di internet per quelli che usano linux. Da una shell account si possono eseguire i comandi principali del linux e fare alcune cose. Oltre alla shell account vi servirà un server dove potrete installarvi

dei programmi dentro come S.A.T.A.N., che potete usare solamente con linux. Se agite attraverso questo server (usando telnet) e attraverso la shell account sarete molto avvantaggiati durante i vostri hackeraggi. Procurarsi una shell account è abbastanza semplice. Ci sono vari modi:

- Controllare se il vostro provider vi ha già dato una shell account. Per fare questo prendete l'ultima parte della vostra email (ad esempio lamer@iol.it prendete iol.it) e connettetevi con telnet a quel server. Usate il vostro login e password per connettervi. Se siete fortunati avete una shell account. Un'altro modo è di connettersi al vostro provider con hyper terminal che si trova in avvio - programmi - accessori - hyperterminal. Connettetevi al numero che usate per connettervi e usate sempre il vostro login e pass. Se vi da un prompt tipo unix allora avete una shell account. Altrimenti potete chiedere all'assistenza tecnica del vostro provider se ne avete già una
- Comprarvi una shell account. La potete richiedere in molti provider piccoli. Non chiedetela a quelli grossi perchè la shell account è lo strumento più utilizzato dagli hacker e quelli, per paura degli hacker, non ve la daranno di certo
- Hackerare una shell account. Questo è relativamente semplice, basta beccare un provider e hackerarlo. Spero che sappiate già come fare;-)
- Farvi dare una shell account da un altro hacker

Per trovare invece un server decente dove potete installare programmi grossi basta beccare un sito internet un po' piccolino (non troppo se no non hackerate un server ma una schifezza) e hackerarlo.

Exploits:

Gli exploits sono dei programmi eseguibili o compilabili scritti in C (spiego dopo..) che aiutano l'hacker ad entrare nel server, ad avere il root o a non essere beccato. Questi file alcune volte sono indispensabili durante un hackeraggio quando il server è molto ben protetto e non riuscite ad hackerarlo con le tecniche tradizionali. Gli script C e gli exploit devono essere sempre lanciati o da una shell account o dal root di un server o dal sito da hackerare. Ci sono moltissimi tipi di script C ed exploit ma i più comuni sono gli sniffer. Gli sniffer sono generalmente degli script che, se lanciati dal sito da hackerare, registrano su un file di log nascosto tutti i login e password di quelli che entrano nel server. Gli sniffer li potete trovare di vari tipi con una piccola ricerca su internet. Per compilare gli script prima si mettono sul server via ftp con il comando PUT e poi si compilano con telnet con il comando cc. Certe volte però i siti dove compilate questi script non hanno tutte le librerie necessarie (per vedere quali librerie servono guardare nel C quali "#include libreria.h" ci sono). In questo caso dovrete mettere voi stessi le librerie necessarie nel server scaricando quelle di un altro sito (con ftp comando GET) oppure compilando lo script su una shell account per C e poi uploadare il file eseguibile sul sito da hackerare e lanciarlo in background. Molti exploit li trovate su www.rootshell.com.

Denial of service:

I programmi denial of service (dos) sono quei programmi che, come dice il nome, negano un dato servizio all'utente. Si usano soprattutto durante le guerre tra hackers e crackers e certe volte danneggiano anche molte altre persone oltre a quelli che combattono. E' molto pericoloso usare questi programmi su dei server poichè essi potrebbero non gradire, loggarvi e denunciarvi al vostro provider quindi usateli con cautela. Questi sono i tipi di dos più comuni.

*Nuke:

I nukers sono dei programmi che sfruttano una vecchia bug di win95 e connettendosi alla porta 139 di un computer windows e mandando una stringa OOB (out of band) lo fanno crashare. Questi programmi non funzionano su win98, su win95 con la patch vtcpupd e su win95 con un antinuke installato.

*Flood:

I flooders sono programmi che sfruttano il PING, cioè un sistema per controllare la velocità tra due server usando la porta 7 ICMP. Quando si pinga si manda un pacchetto (un piccolo pezzo di dati) e si calcola il tempo che si impiega a riceverlo. Il flood manda enormi pacchetti di ping a grande velocità rallentando la connessione della vittima. Alcuni flood usano il protocollo UDP e mandano solo tanti pacchetti ma non impegnano il pc a rispondere. Il ping flood è il più efficace.

*Mailbomb:

I mailbomber sono dei programmi che usano tanti server per inviare mail e inviano centinaia o migliaia di mail uguali ad un indirizzo email. Questi programmi possono anche danneggiare i server utilizzati poichè li rallentano molto e riempiono i loro file di log e certe volte un server o due può crashare.

*Smurf:

Lo smurf è per me il più versatile, efficace e mortale dos tra tutti quelli esistenti. E' come un ping flood ma fa in modo che la sua velocità venga centuplicata o peggio. Come è possibile?? Semplice. Ci sono dei server chiamati server di broadcast che se vengono pingati essi rispondono tante volte quante sono le macchine a cui sono connessi. Certe volte rispondono centinaia o addirittura (in casi molto rari) decine di migliaia di volte. Ma voi direte: embè?? Sono io che pingo questi server e non la vittima!! Vi sbagliate. Spoofando i pacchetti ICMP (cioè cambiandone l'ip di provenienza) è possibile ingannare il server e fargli credere che il ping provenga da un'altra parte. A questo punto le cose sono molto semplici. Ci facciamo una lista di broadcast con UBS (per win) o con broadscan (per linux), prendiamo smurf o winsmurf e lo usiamo. Esso manderà tantissimi pacchetti a velocità altissima in modo da occupare molta della banda del nostro modem. Manderà un pacchetto per server in ordine di successione e ricomincerà da capo ogni volta. Il risultato è che la vittima riceve dieci, cento, mille volte (a seconda del numero medio di risposte dei nostri broadcast) i pacchetti che mandiamo noi, causandone l'esclusione parziale (se la vittima è un server potente e grosso) o totale (se è un normale utente client) dalla rete.

*Vari:

Ci sono molti altri tipi di dos. Alcuni di questi sono:

- ICQbomb
- IRCkill
- PowWowflood
- Ssping
- Jolt
- IceNuke
- Bouncer
- Pepsi
- UDP flood
- Suffer
- Land
- Teardrop
- Bonk
- Boink
- NesTea
- PortFuck

Potete trovare informazioni su questi dos con qualche ricerca su internet.

Trucchetti vari:

Questi sono alcuni trucchetti che conosco. Sono pochi ma ne aggiungerò degli altri. Di solito funzionano su sistemi vecchi o deboli quindi non vi assicuro niente.

- Provate il trucchetto del "quote". Connettetevi via ftp al server da hackerare. Quando vi chiede login e pass premete sempre invio. Poi scrivete:

  > quote user ftp
  User OK send password.
  >quote cwd ~root

...
>quote pass ftp

Avrete il root

- Provate il trucchetto del frontpage. Se nel sistema è installato frontpage prendete il .pwd nella directory del fp. Conterrà la password criptata in DES (se quella del root è shadowata può servire)

File di LOG:

I file di log sono i file dove vengono registrati alcune o tutte le attività nel server. I file di log che interessano agli hacker sono quelli dove vengono registrati i login falliti, upload di file e log che potrebbero far scoprire al sysop la vostra presenza.
I file di log più comuni sono:

- /usr/adm/sulog o /usr/adm/su_log
- /usr/adm/loginlog o /usr/adm/acct/loginlog
- /usr/adm/errlog
- /usr/adm/culog

Ricordate di EDITARE questi file, NON di cancellarli.

S.A.T.A.N.:

Il S.A.T.A.N. (Security Administration Tool for Analyzing Networks) è un programma che gira sotto unix con perl 5 che scannerizza un network cercando di trovare delle falle e dei bug. E' provvisto di un grosso manuale in html quindi non perdo tempo a spiegarvi come si usa. Bisogna usare una shell account o linux per lanciarlo e richiede una buona velocità di connessione. Per controllare se un server è stato attaccato dal SATAN si possono usare due programmi, il gabriel e il courtney. In teoria questo programma servirebbe a controllare la propria rete e a correggere le aperture che il satan trova. Ma sono sicuro che troverete un altro modo d'uso per questo simpatico prog=). Per trovarlo basta fare una piccola ricerca, di solito il file che lo contiene si chiama satan-1.1.1.tar.Z.

Port surfing:

Il port surfing è una tecnica di penetrazione dei sistemi. Consiste nel fare un portscan (spiego dopo) ad un server e di provare ad acquisire più informazioni possibili da ogni porta che risulta aperta. Il portscanner si può trovare sempre con una piccola ricerca, il mio portscanner preferito è il 7th Sphere Portscan, molto veloce. Il portscanner si connette a tutte le porte una ad una dalla porta 0 alla 65536 e ti avverte quando una porta è aperta. In questo modo tu puoi sapere tutte le porte aperte ed eventualmente segrete in un server e connetterti cercando informazioni. Ad esempio mi è capitato una volta che stavo facendo un portscan su un server e ho trovato una porta aperta con valore molto elevato, intorno a 30000. Mi sono connesso a quella porta (con telnet specificando il numero quando fai connetti - sistema remoto) e ho provato a scrivere le cose più comuni, tipo HELP, HELO, HELLO, LOGIN. Ho provato root e puf mi ha dato la password. Schifo di server eh? Non vi assicuro che succeda anche a voi cmq. Questo è stato un colpo di fortuna.

Tutorial:

Eccoci alla parte che tutti aspettavate. Il TUTORIAL. Per quelli che non sanno cos'è, il tutorial è una specie di lezione "guidata". In questo caso è un hackeraggio guidato. Naturalmente userò un server inesistente perchè il vostro primo hack dovrete farlo VOI. Cominciamo:

Sono su irc, un amico hacker comincia a rompere che la sua home page è troppo figa etc. Mi viene un'idea di fargli uno scherzetto e visito la sua pagina. Carina sì...facciamo sto scherzo=). Sarebbe bello rinominare index.html in index2.html e metterci un nuovo index.html con scritto "QUESTA PAGINA E' STATA HACKERATA DA KALIDOR - CLICCA QUI PER ENTRARE" o qualcosa di simile. Beh vediamo l'url:

http://www.sardine.com/scatola/index.html

Vediamo un po se esiste sardine.com. Faccio il ping...l'host non esiste. Vuol dire che devo hackerare www.sardine.com. Fingeriamo...

No one connected now.

Vuol dire che non c'è nessuno. Beh proviamo a fingerare sardine.

Login	Name	TTY	Idle	When	Where
sardine	SardineWEB	pts/18		<Sep 1 17:30>	maiden

Bene c'è. Facciamo un po di whois...niente whois. Portscan...porte normali, le solite 21, 23, 25, 79, 80, 110. Ok apriamo ftp.

>Open
(to)www.sardine.com

Connected to www.sardine.com. Ftp version 2.0 on www.sardine.com.
Login:

Mah proviamo sardine no?

Login: sardine
Password:

Beh..proviamoooo....."sardine"! =)

Password:

(Naturalmente non si vede ma li ho scritto sardine).

Login incorrect. Login failed.
>

Azzo. Sbagliato. Beh proviamo il trucco del quote.

>quote user ftp
User name OK send password.
>quote cwd ~root
Please login with USER and PASS

Ok se dice quello il trucco non funziona. Hmm...proviamo maiden...c'era scritto nel finger.

>user sardine
User name OK send password.
Password:
User sardine logged in. Last login <Sep 1 17:30>.
>

MITICO! SONO ENTRATO. Ora chessifa?

>pwd
Current directory is /
>cd etc
>get passwd
Open ASCII mode data connection for /bin/ls
Tranfer complete. Recieved 9345 bytes in 2.3 seconds.
>

Ok vediamo un po sto passwd file. Apro... AZZ CI SONO 150 LOGIN TUTTI CRIPTATI DES!!! E ANCHE IL ROOT E' CRIPTATO DES. MITICO!!!

>bye
Goodbye.

Ok prendiamo John The Ripper. Proviamo tutto.

john -single passwd
john -wordlist password.txt -rules passwd
john -i:alpha passwd
john -i:digits passwd
john -i passwd

A questo punto abbiamo 138 login..così dice il john...vediamo un po. Quello che all'inizio ci interessava, scatola non l'abbiamo..vabbè. Cerchiamo un po root...il codice è `Ko./GkA9YUfFA ...` ROOT! ECCOLO!

`Ko./GkA9YUfFA:`alskdjfh

A noi! Connettiamoci con telnet...editiamo il password file e aggiungiamo una backdoor...ci togliamo dai log file...unshadowiamo i login che erano shadowati...
Ora possiamo giocherellare con la pagina del mio amico e in più abbiamo un bel server tutto nostro..slurp. Ricordiamoci però di non modificare niente altro...e ricordiamoci che il sito del tizio che hackeriamo è di uno che sa stare agli scherzi...cioè non dirà a quelli del provider che la sua pagina è stata hackerata. Se no vi beccano...capito? Se volete hackare il sito di uno che non conoscete non cambiate NULLA.

Conclusione:

La guida è finita. Sigh. Vabbè cmq se l'avete letta tutta vi aspettano molte giornate & nottate divertenti di hackeraggi...capirete ben presto quanto sia bello e imparerete moltissime cose. Magari scriverete anche voi una guida ancora migliore della mia...non si sa mai=). Spero che vi sia piaciuta e gradirei molto qualche mail..kalidor@tin.it. Se sono mailbomb o flames mandateli a dev/null@tin.it (dev/null è il posto dove vengono conservati gli archivi vecchi destinati a perdersi nel tempo). Contattatemi anche con ICQ il mio uin è 7874185. Mi trovate a chattare su kali in Tin Kali Server con il nickname {FICT}Kalidor (indovinate cosa vuol dire FICT) e su IRC con il nick Kalidor.
Ricordatevi di visitare la mia homepage a http://kalidor.tsx.org
Lì troverete tutto ciò di cui avrete bisogno. Grazie di aver letto la mia guida e HAPPY HACKING!!!! HACK THE WORLD!!!!!!!!